UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,566	05/10/2001	Takuya Oshima	112857-245	6260

29175 7590 06/10/2005

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

EXAMINER	
WORJLOH, JALATEE	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/852,566	OSHIMA ET AL.	
	Examiner	Art Unit	
	Jalatee Worjloh	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1- 17 and 19-28* is/are pending in the application.

4a) Of the above claim(s) *8,9,15 and 16* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,10-14,17 and 19-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This Office Action is responsive to the amendment filed February 14, 2005, in which claims 1, 5, 13, 17, 19, and 22 were amended and claim 18 canceled.

Response to Arguments

2. Applicant's arguments with respect to claims 1, 17 and 22 are have been considered but are moot in view of the new ground(s) of rejection.

3. Applicant's arguments filed February 14, 2005 have been fully considered but they are not persuasive.

Applicant argues that Mansvelt does not teach or suggest a settlement management device for managing settlement between the storage device and the store device or transmitting the settlement information subjected to the encryption processing to the client device or funds transfer machine where the client device outputs the settlement information received from the settlement management device to the data storage device. The examiner disagrees; Mansvelt teaches a retailer point of sale device (POS), which is a store device for providing transactional services, a data storage device (i.e. the user's smart card) and a settlement management device, which is the financial institution FTM. The financial institution FRM settles the account by crediting the retailer's account and debiting the cardholder account. As for transmitting the information subjected to encryption processing to the client device, Mansvelt discloses the FTM routing the encrypted data to the client card. Notice, it is known that in order for the card to

receive the data it must be inserted into a client device. Thus, the process of transmitting the encrypted information to the client device is an inherent step.(see col. 3, lines 40-43).

4. Claims 1-7, 10-14,17, and 19-28 have been examined.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 10 and 24-27 are rejected under 35 U.S.C. 102(b) as being anticipated by European Patent NO. 042180 A2 to Mansvelt.

Referring to claim 10, Mansvelt et al. disclose a settlement information creation part (i.e. financial institution's FTM) for creating, based on settlement request information from the store device (i.e. retailer's POS), settlement information for making settlement by the data storage device (i.e. "smart card"), a settlement information encryption part (FTM) for subjecting the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device and a settlement information output part (FTM) for outputting the settlement information subjected to the encryption processing to

the data storage device through a client device provided with an information input and output function to the data storage device (see col. 4, lines 34-46 & col. 6, lines 32-56).

Referring to claim 24, Mansvelt et al. disclose a settlement information receiver part (i.e. smart card) for receiving settlement information, which is created by the settlement management device (i.e. FTM) based on settlement request information from the store device (i.e. retailer's POS) and is subjected to an encryption processing by using a common key shared by the settlement management device and the data storage device (i.e. smart card) and a settlement information output part (i.e. FTM) for outputting the settlement information received from the settlement management device to the data storage device (see col. 4, lines 34-46; col. 6, lines 32-56).

Referring to claims 25 and 26, Mansvelt et al. disclose a device for inputting settlement information, which is created by the settlement management device based on settlement request information from the store device and is subjected to an encryption processing by using a common key shared by the settlement management device and the data storage device, through a client device provided with an information input and output function to the data storage device, wherein the data storage device is an IC card (see col. 4, lines 34-46; col. 6, lines 32-56).

Referring to claim 27, Mansvelt et al. disclose creating settlement information for making settlement by the data storage device storing value information, based on settlement request information from the store device, subjecting the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device (see col. 4, lines 34-46; col. 6, lines 32-56).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 6834271 to Hodgson et al. in view of by European Patent No. 0421808 A2 to Mansvelt et al.

Hodgson et al. disclose a data storage device (i.e. credit cards or debit cards) in which value information is stored, a client device (i.e. PIN pad) provided with an information input and output function to the data storage device (see col. 4, lines 51-64 The PIN/Pad is used to conduct secure financial transaction for credit cards or debit cards), a store device (i.e. merchants' web server) for providing at least one of commodities and services (col. 5, lines 4-9), a settlement device (i.e. secure transaction manager server) for managing settlement between the data storage device and the store device (see col. 5, lines 10-34), a communication system (i.e. a communication interface) for connecting the client device, the store device, and the settlement management device so as to enable bi-directional communication between the client device, the store device and the settlement management device (see col. 13, lines 16-34) and wherein the settlement management device creates, based on settlement request information from the store device, settlement information for making settlement by the data storage device (see col. 6, lines 29-37 the secure transaction management system decrypts, formats and routes a payment request

to the banking system). Hodgson et al. do not expressly disclose the settlement management device subjects the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device, and transmits the settlement information subjected to encryption processing to the client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device. Mansvelt et al. disclose the settlement management device (i.e. financial institution's FTM) subjects the settlement information to an encryption processing by using a common key (i.e. issuer key) shared by the settlement management device and the data storage device (i.e. smart card), and transmits the settlement information subjected to encryption processing to the client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device (see col. 6, lines 32-56). Notice, Mansvelt discloses the FTM routing the encrypted data to the client card. It is known in the art that the in order for the card to receive the data it must be inserted into a client device. Thus, the process of transmitting the encrypted information to the client device is an inherent step (see col. 3, lines 40-43). At the time the invention of was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Hodgson et al. to include a settlement management device that subjects the settlement information to an encryption processing by using a common key shared by the settlement management device and the data storage device, and transmits the settlement information subjected to encryption processing to the client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device. One of ordinary skill in the art would have been motivated to do this because it provides data security.

9. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hodgson et al. and Mansvelt et al. as applied to claim 1 above, and further in view of US Patent No. 637578 to Linehan.

Referring to claims 2 and 3, Hodgson et al. disclose a store device, and a settlement management device (see claims 1 and 10 above). Hodgson et al. do not expressly disclose the store device creates a first signature indicating validity of the settlement request information by using a private key of the store device and transmits the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store. Linehan discloses the store device (i.e. "merchant's computer") creates a first signature (i.e. "merchant digital signature") indicating validity of the settlement request information by using a private key of the store device and transmits the settlement request information with the first signature to the settlement management device (i.e. "issuer gateway operating on behalf of an issuing bank"), and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store, wherein the settlement request information with the first signature is transmitted to the settlement management device through the client device (i.e. "consumer's computer") (see col. 4, lines 10-28; col. 2, lines 40-42). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Hodgson et al. to allow the store device to create a first signature indicating validity of the settlement request information by using a private key of the store device and transmit the settlement request information with the first signature to the

settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of security and prevents unauthorized individuals from access the settlement request.

10. Claims 4- 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hodgson et al., Mansvelt et al., Linehan as applied to claim 1 above, and further in view of Takayama.

Referring to claim 4, Hodgson et al. disclose a settlement management device and a client device (see claim 2). Hodgson et al. do not expressly disclose the settlement management device creates a second signature indicating validity of the settlement information with the first signature by using a private key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device, and wherein the client device checks validity of the second signature received from the settlement management device by using a public key corresponding to the private key of the settlement management device, and then outputs the settlement information to the data storage device. Linehan discloses the settlement management device creates a second signature (i.e. the issuer gateway's signature) indicating validity of the settlement information with the first signature by using a private key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device (see col. 4, lines 24-41). Takayama discloses the client device checks validity of the second signature received from the settlement management device by using a public key

corresponding to the private key of the settlement management device, and then outputs the settlement information to the data storage device (see paragraph [0111], lines 22-28 the process of authenticating the digital signature can be efficiently performed in parallel by the user information processing means). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Hodgson et al. to allow the settlement management device to create a second signature indicating validity of the settlement information with the first signature by using a private key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device, and wherein the client device checks validity of the second signature received from the settlement management device by using a public key corresponding to the private key of the settlement management device, and then outputs the settlement information to the data storage device. One of ordinary skill in the art would have been motivated to do this because it provides superior safety and convenience by preventing unauthorized individuals from accessing transmitted data (see Takayama, paragraph [0020]).

Referring to claim 5, Hodgson et al. disclose a settlement management device and a store device, the settlement management device creates settlement completion information (see claim 1 above). Hodgson et al. do not expressly disclose the settlement management device creates a third signature indicating validity of the settlement completion information by using the private key of the settlement device, and transmits the settlement completion information including the settlement information and given the third signature to the store device, and wherein the store

device checks validity of the third signature received from the settlement management device by using the public key corresponding to the private key of the settlement management device. Linehan discloses the settlement management device (i.e. "issuing bank") creates settlement completion information, creates a third signature indicating validity of the settlement completion information (i.e. "authorization token") by using the private key of the settlement device, and transmits the settlement completion information including the settlement information and given the third signature to the store device (i.e. "merchant's computer"), and wherein the store device checks validity of the third signature received from the settlement management device by using the public key corresponding to the private key of the settlement management device (see col. 4, lines 31-44; col. 8, lines 63-65; col. 2, lines 40-42). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Hodgson et al. to allow the settlement management device to create settlement completion information, create a third signature indicating validity of the settlement completion information by using the private key of the settlement device, and transmit the settlement completion information including the settlement information and given the third signature to the store device, and wherein the store device checks validity of the third signature received from the settlement management device by using the public key corresponding to the private key of the settlement management device. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of security and prevents unauthorized individuals from access the settlement data.

Referring to claim 6, Hodgson et al. disclose a store device and a client device (see claim 5 above). Hodgson et al. do not expressly disclose the store device receives the settlement

completion information with the third signature, creates settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmits the settlement completion receipt information with the fourth signature to the client device, and wherein the settlement management device and the client device check validity of the fourth signature received from the store device by using a public key corresponding tot the private key of the store device. Takayama discloses the store device (i.e. "the credit settlement terminal") receives the settlement completion information with the third signature, creates settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmits the settlement completion receipt information with the fourth signature to the client device (see paragraphs [0812]-[0814] upon receipt of the clearing confirmation notification, the credit settlement terminal decrypts it, examines the digital signature...the credit settlement terminal generates a receipt and transmits it to the service providing system...a digital signature of a merchant is provided for data consists of a receipt header ...the service providing system decrypts it, examines the digital signature, and transmits a receipt to the personal credit terminal) and wherein the settlement management device and the client device (i.e. "personal credit terminal") check validity of the fourth signature received from the store device by using a public key corresponding tot the private key of the store device (see paragraph [0111], lines 22-28 the process of authenticating the digital signature can be efficiently performed in parallel by the user information processing means). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Hodgson et al. to allow store device to receive the settlement completion information with the third signature, create settlement completion information receipt information with a

fourth signature by using a private key of the store device, and transmit the settlement completion receipt information with the fourth signature to the client device, and wherein the settlement management device and the client device check validity of the fourth signature received from the store device by using a public key corresponding tot the private key of the store device. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of data security, thereby preventing unauthorized individuals from accessing the transmitted data.

11. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hodgson et al. and Mansvelt et al. as applied to claim 1 above, and further in view of US Patent No. 6338050 to Conklin et al.

Hodgson et al. disclose a store device (see claim 1 above). Mansvelt et al. do not expressly disclose the store device is a mall including a plurality of lower store devices. Conklin et al. disclose a settlement system including a store device, which is a mall including a plurality of lower store devices (see col. 2, lines 64-67). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Hodgson et al. to include a mall including a plurality of lower store devices. One of ordinary skill in the art would have been motivated to do this because it provides versatility by allowing the user to shop at various stores.

12. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansvelt et al. as applied to claim 10 above, and further in view of Linehan.

Mansvelt et al. disclose a store device, and a settlement management device (see claim 10 above). Mansvelt et al. do not expressly disclose the store device creates a first signature indicating validity of the settlement request information by using a private key of the store device and transmits the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store. Linehan discloses the store device (i.e. "merchant's computer") creates a first signature (i.e. "merchant digital signature") indicating validity of the settlement request information by using a private key of the store device and transmits the settlement request information with the first signature to the settlement management device (i.e. "issuer gateway operating on behalf of an issuing bank"), and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store, wherein the settlement request information with the first signature is transmitted to the settlement management device through the client device (i.e. "consumer's computer") (see col. 4, lines 10-28; col. 2, lines 40-42). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Mansvelt et al. to allow the store device to create a first signature indicating validity of the settlement request information by using a private key of the store device and transmit the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store. One of

ordinary skill in the art would have been motivated to do this because it provides an additional level of security and prevents unauthorized individuals from access the settlement request.

13. Claims 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mansvelt et al. and Linehan as applied to claim 11 above, and further in view of Takayama.

Referring to claim 12, Mansvelt et al. disclose a settlement management device and a client device (see claim 10 above). Mansvelt et al. do not expressly disclose the settlement management device creates a second signature indicating validity of the settlement information with the first signature by using a private key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device, and wherein the client device checks validity of the second signature received from the settlement management device by using a public key corresponding to the private key of the settlement management device, and then outputs the settlement information to the data storage device. Linehan discloses the settlement management device creates a second signature (i.e. the issuer gateway's signature) indicating validity of the settlement information with the first signature by using a private key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device (see col. 4, lines 24-41). Takayama discloses the client device checks validity of the second signature received from the settlement management device by using a public key corresponding to the private key of the settlement management device, and then outputs the settlement information to the data storage device (see paragraph [0111], lines 22-28 the process of authenticating the digital signature can be efficiently performed in parallel by the user information processing means). At the time the invention was

made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Mansvelt et al. to allow the settlement management device to create a second signature indicating validity of the settlement information with the first signature by using a private key of the settlement management device, and transmits the settlement information given the second signature and subjected to the encryption processing to the client device, and wherein the client device checks validity of the second signature received from the settlement management device by using a public key corresponding to the private key of the settlement management device, and then outputs the settlement information to the data storage device. One of ordinary skill in the art would have been motivated to do this because it provides superior safety and convenience by preventing unauthorized individuals from accessing transmitted data (see Takayama, paragraph [0020]).

Referring to claim 13, Mansvelt et al. disclose a settlement management device and a store device, the settlement management device creates settlement completion information (see claim 12 above). Mansvelt et al. do not expressly disclose the settlement management device creates a third signature indicating validity of the settlement completion information by using the private key of the settlement device, and transmits the settlement completion information including the settlement information and given the third signature to the store device, and wherein the store device checks validity of the third signature received from the settlement management device by using the public key corresponding to the private key of the settlement management device. Linehan discloses the settlement management device (i.e. "issuing bank") creates settlement completion information, creates a third signature indicating validity of the

settlement completion information (i.e. "authorization token") by using the private key of the settlement device, and transmits the settlement completion information including the settlement information and given the third signature to the store device (i.e. "merchant's computer"), and wherein the store device checks validity of the third signature received from the settlement management device by using the public key corresponding to the private key of the settlement management device (see col. 4, lines 31-44; col. 8, lines 63-65; col. 2, lines 40-42). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Hodgson et al. to allow the settlement management device to create settlement completion information, create a third signature indicating validity of the settlement completion information by using the private key of the settlement device, and transmit the settlement completion information including the settlement information and given the third signature to the store device, and wherein the store device checks validity of the third signature received from the settlement management device by using the public key corresponding to the private key of the settlement management device. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of security and prevents unauthorized individuals from access the settlement data.

Referring to claim 14, Mansvelt et al. disclose a store device and a client device (see claim 13 above). Hodgson et al. do not expressly disclose the store device receives the settlement completion information with the third signature, creates settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmits the settlement completion receipt information with the fourth signature to the client device, and wherein the settlement management device and the client device check validity of

the fourth signature received from the store device by using a public key corresponding tot the private key of the store device. Takayama discloses the store device (i.e. "the credit settlement terminal") receives the settlement completion information with the third signature, creates settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmits the settlement completion receipt information with the fourth signature to the client device (see paragraphs [0812]-[0814] upon receipt of the clearing confirmation notification, the credit settlement terminal decrypts it, examines the digital signature...the credit settlement terminal generates a receipt and transmits it to the service providing system...a digital signature of a merchant is provided for data consists of a receipt header ...the service providing system decrypts it, examines the digital signature, and transmits a receipt to the personal credit terminal) and wherein the settlement management device and the client device (i.e. "personal credit terminal") check validity of the fourth signature received from the store device by using a public key corresponding tot the private key of the store device (see paragraph [0111], lines 22-28 the process of authenticating the digital signature can be efficiently performed in parallel by the user information processing means). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Mansvelt et al. to allow store device to receive the settlement completion information with the third signature, create settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmit the settlement completion receipt information with the fourth signature to the client device, and wherein the settlement management device and the client device check validity of the fourth signature received from the store device by using a public key corresponding tot the private key of the

store device. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of data security, thereby preventing unauthorized individuals from accessing the transmitted data.

14. Claims 17,19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linehan in view of Mansvelt.

Linehan discloses a settlement request information creation part (i.e. "merchant's computer") for creating settlement request information, a first signature creation part (i.e. "merchant's computer") indicating validity of the settlement request information by using a private key of the store device (i.e. "merchant's computer"), and a settlement request information transmission part (i.e. "consumer's computer") for transmitting the settlement request information with the first signature to the settlement management device (i.e. "issuing bank") which can check validity of the first signature by using a public key corresponding to the private key of the store device and transmitting the settlement information (i.e. authorization token) subjected to the encryption processing to a client device (i.e. consumer computer) when the validity of the first signature is verified by the settlement management device (see col. 4, lines 10-28; col. 2, lines 40-42) Linehan does not expressly disclose a settlement information creation part for creating settlement information to make settlement by the data storage device, an encryption part for encrypting the settlement information using common key shared by the settlement management device and the data storage device, wherein the client device outputs the settlement information received from the settlement management device to the data storage device. Mansvelt et al. disclose a settlement information creation part (i.e. financial institution FTM) for creating settlement information (i.e. message which include amount to be transferred,

TSN and USN) to make settlement by the data storage device (i.e. smart card), an encryption part (the financial institution's machine...notice the amount of the transfer, together with the TSN and the USN, is encrypted under the issuer key of the financial institution) for encrypting the settlement information using common key shared by the settlement management device and the data storage device, wherein the client device outputs the settlement information received from the settlement management device to the data storage device (see col. 6, lines 32-56). At the time the invention of was made, it would have been obvious to a person of ordinary skill in the art to modify the device disclose by Linehan to include a settlement information creation part for creating settlement information to make settlement by the data storage device, an encryption part for encrypting the settlement information using common key shared by the settlement management device and the data storage device, wherein the client device outputs the settlement information received from the settlement management device to the data storage device. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of data security, thereby preventing unauthorized individuals from accessing the transmitted data.

Referring to claim 19, Linehan discloses the settlement management device (i.e. "issuing bank") creates, based on the settlement request information from the store device (i.e. "merchant's computer"), settlement information (i.e. "authorization token") for making settlement (see col. 4, lines 31-38), wherein the settlement request information with the first signature is transmitted from the store device to the settlement management device through a client device (see col. 4, lines 10-23). Linehan does not expressly disclose settlement information for making settlement by the data storage device, subjects the settlement information

to the encryption processing to a client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device. Mansvelt et al. disclose settlement information for making settlement by the data storage device, subjects the settlement information to the encryption processing to a client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device (see col. 4, lines 34-46; col. 6, liens 32-56). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the device disclose by Linehan to include settlement information for making settlement by the data storage device, subjects the settlement information to the encryption processing to a client device, and wherein the client device outputs the settlement information received from the settlement management device to the data storage device. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of security.

Referring to claim 20, Linehan discloses the settlement management device (i.e. "issuing bank") creates settlement completion information, creates a third signature indicating validity of the settlement completion information (i.e. "authorization token") by using the private key of the settlement device, and transmits the settlement completion information including the settlement information and given the third signature to the store device (i.e. "merchant's computer"), and wherein the store device checks validity of the third signature received from the settlement management device by using the public key corresponding to the private key of the settlement management device (see col. 4, lines 31-44; col. 8, lines 63-65; col. 2, lines 40-42).

15. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Linehan and Mansvelt et al. as applied to claim 20 above, and further in view of Takayama.

Linehan discloses the store device receives the settlement completion information (i.e. "authorization token") with the third signature (see col. 4, lines 31-40). Linehan does not expressly disclose the store device creates settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmits the settlement completion receipt information with the fourth signature to the client device, and wherein the settlement management device and the client device check validity of the fourth signature received from the store device by using a public key corresponding to the private key of the store device. Takayama discloses the store device (i.e. "the credit settlement terminal") creates settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmits the settlement completion receipt information with the fourth signature to the client device (see paragraphs [0812]-[0814]) and wherein the settlement management device and the client device (i.e. "personal credit terminal") check validity of the fourth signature received from the store device by using a public key corresponding tot the private key of the store device (see paragraph [0111], lines 22-28). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Linehan to allow store device to create settlement completion information receipt information with a fourth signature by using a private key of the store device, and transmit the settlement completion receipt information with the fourth signature to the client device, and wherein the settlement management device and the client device check validity of the fourth signature received from the store device by using a public key corresponding tot the private key

of the store device. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of data security, thereby preventing unauthorized individuals from accessing the transmitted data.

16. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mansvelt et al. as applied to claim 27 above, and further in view of Linehan.

Mansvelt et al. disclose a store device, and a settlement management device (see claim 27 above). Mansvelt et al. do not expressly disclose the store device creates a first signature indicating validity of the settlement request information by using a private key of the store device and transmits the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store. Linehan discloses the store device (i.e. "merchant's computer") creates a first signature (i.e. "merchant digital signature") indicating validity of the settlement request information by using a private key of the store device and transmits the settlement request information with the first signature to the settlement management device (i.e. "issuer gateway operating on behalf of an issuing bank"), and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store, wherein the settlement request information with the first signature is transmitted to the settlement management device through the client device (i.e. "consumer's computer") (see col. 4, lines 10-28; col. 2, lines 40-42). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the system disclose by Mansvelt et al. to allow the store device to create a first signature indicating validity of the

settlement request information by using a private key of the store device and transmit the settlement request information with the first signature to the settlement management device, and wherein the settlement management device checks validity of the first signature received from the store device by using a public key corresponding to the private key of the store. One of ordinary skill in the art would have been motivated to do this because it provides an additional level of security and prevents unauthorized individuals from access the settlement request.

As for claim 22, see claim 17's rationale above.

As for claim 23, see claim 1's rationale above.

Conclusion

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jalatee Worjloh whose telephone number is (571)272-6714. The examiner can normally be reached on Mondays-Thursdays 8:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (571)272-6712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306 for Regular/After Final Actions and (571)273-6714 for Non-Official/Draft.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Jalatee Worjloh
Patent Examiner
Art Unit 3621

***
June 6, 2005